

LEVERAGING SOCIAL NETWORKING IN THE UNITED STATES ARMY

BY

COLONEL JIMMY L. HALL, JR.
United States Army

DISTRIBUTION STATEMENT A:

Approved for Public Release.
Distribution is Unlimited.

USAWC CLASS OF 2011

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.



U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

| REPORT DOCUMENTATION PAGE | | | | Form Approved OMB No. 0704-0188 | |
|---|-----------------------------|---|---|--|---|
| Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS. | | | | | |
| 1. REPORT DATE (DD-MM-YYYY) 16-03-2011 | | 2. REPORT TYPE Strategy Research Project | | 3. DATES COVERED (From - To) | |
| 4. TITLE AND SUBTITLE Leveraging Social Networking in the United States Army | | | | 5a. CONTRACT NUMBER | |
| | | | | 5b. GRANT NUMBER | |
| | | | | 5c. PROGRAM ELEMENT NUMBER | |
| 6. AUTHOR(S) Colonel Jimmy L. Hall, Jr. | | | | 5d. PROJECT NUMBER | |
| | | | | 5e. TASK NUMBER | |
| | | | | 5f. WORK UNIT NUMBER | |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Colonel Steve Sobotta Department of Command, Leadership, & Management | | | | 8. PERFORMING ORGANIZATION REPORT NUMBER | |
| 9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Army War College 122 Forbes Avenue Carlisle, PA 17013 | | | | 10. SPONSOR/MONITOR'S ACRONYM(S) | |
| | | | | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) | |
| 12. DISTRIBUTION / AVAILABILITY STATEMENT Distribution A: Unlimited | | | | | |
| 13. SUPPLEMENTARY NOTES | | | | | |
| 14. ABSTRACT In 2007, the U. S. Department of Defense (DoD) began blocking social networking sites such as including YouTube and MySpace from its computer networks based on concerns for bandwidth, network security, and posting of personal and operational information. In February 2010, the Department issued a memorandum that set a new policy allowing access to social-networking services (SNS) from its network. The policy allows all users of unclassified computers in the .mil domain access to some of the more popular SNSs including Facebook, Twitter, Flickr and YouTube. The Army issued its policy immediately afterwards, requiring all Army Commands to configure their networks to allow for the full range of social networking capabilities. This paper briefly defines social networking, studies the history of social networking, speaks to how social networking can serve as a change agent within the Army, analyzes the risks and challenges of lifting the ban on SNSs, and finally, states the benefits of leveraging social networking in the Army. Leveraging social networking is a good idea. Social Networking will continue to provide an indisputable influence on our department's organizational beliefs, and values, and have a positive effect on soldier moral, unit climates, information sharing, collaboration, crisis and strategic communications. | | | | | |
| 15. SUBJECT TERMS Social Media, Networks | | | | | |
| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT UNLIMITED | 18. NUMBER OF PAGES 26 | 19a. NAME OF RESPONSIBLE PERSON |
| a. REPORT UNCLASSIFIED | b. ABSTRACT UNCLASSIFIED | c. THIS PAGE UNCLASSIFIED | | | 19b. TELEPHONE NUMBER (include area code) |

USAWC STRATEGY RESEARCH PROJECT

LEVERAGING SOCIAL NETWORKING IN THE UNITED STATES ARMY

By

Colonel Jimmy L. Hall, Jr.
United States Army

Colonel Steve Sobotta
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Colonel Jimmy L. Hall, Jr.
TITLE: Leveraging Social Networking in the United States Army
FORMAT: Strategy Research Project
DATE: 16 March 2011 WORD COUNT: 5,101 PAGES: 26
KEY TERMS: Social Media, Networks
CLASSIFICATION: Unclassified

In 2007, the U. S. Department of Defense (DoD) began blocking social networking sites such as including YouTube and MySpace from its computer networks based on concerns for bandwidth, network security, and posting of personal and operational information. In February 2010, the Department issued a memorandum that set a new policy allowing access to social-networking services (SNS) from its network. The policy allows all users of unclassified computers in the .mil domain access to some of the more popular SNSs including Facebook, Twitter, Flickr and YouTube. The Army issued its policy immediately afterwards, requiring all Army Commands to configure their networks to allow for the full range of social networking capabilities. This paper briefly defines social networking, studies the history of social networking, speaks to how social networking can serve as a change agent within the Army, analyzes the risks and challenges of lifting the ban on SNSs, and finally, states the benefits of leveraging social networking in the Army. Leveraging social networking is a good idea. Social Networking will continue to provide an indisputable influence on our department's organizational beliefs, and values, and have a positive effect on soldier moral, unit climates, information sharing, collaboration, crisis and strategic communications.

LEVERAGING SOCIAL NETWORKING IN THE UNITED STATES ARMY

We use social media just as other organizations do. It's a critical element for us.¹

—Deputy Defense Secretary William J. Lynn III

Over the past five years, social networking has grown from a quiet and collegiate way for mostly teens and young adults to communicate to imaginably the future of how people share information and share of themselves. It has truly been amazing to see how much the Internet business has evolved as a result of Facebook, MySpace, Twitter, and other social media technologies.² Since the start of social networking sites (SNSs), sites such as MySpace and Facebook have appealed to millions of people, many of whom have incorporated visiting these sites into their everyday lives.

There are thousands of SNSs supporting a varied array of interests and practices and, although they share basic technological features, the ethos that develops around SNSs is wide-ranging. For instance, most sites support current or established social networks, while others service visitors or guests connected by common interests, political opinions, or community activities. Some SNSs cater to miscellaneous audiences; while others are constructed to people based on a common language, or shared racial, sexual, religious, or nationality-based identities. Moreover, social networking sites differ in the scope to which they incorporate novel information and communication tools, such as portable connectivity devices, blogging, or picture and other audiovisual sharing methods.

Several years ago, the United States Department of Defense (DoD) initiated blocking access to social networking sites such as MySpace, Facebook, and YouTube from its computer networks based on concerns for bandwidth, network security, and

posting of personal and operational information. After a nearly three year ban on access to social networking, and an ever growing popularity in SNSs, the Department relaxed its policy. Specifically, in February 2010, the Department issued a memorandum that sets a new policy allowing access to social-networking services from its network.³ The new policy further dictates that if your organization has a SNS such as a Facebook page, then it's referred to as an 'official external presence' and must be registered with the Assistant Secretary of Defense for Public Affairs.

The news of this announcement broke on the Twitter feed of Price Floyd, the Principal Deputy Assistant Secretary of Defense for Public Affairs, and not via a traditional press release. The new policy seeks to balance the needs of troops to connect with their loved ones via social media while also maintaining an appropriate level of security. As the policy goes into effect, DoD will require all military units to remove the social sites from their internal "blacklist." (A blacklist is an access control system which denies entry to a specific list of users, programs, or network addresses).

In implementing the new policy, the department also launched its own social media hub, a blog-like site complete with live Twitter feeds, Tweet-me buttons and "share on Facebook" links.⁴ According to the Times, Lindy Kyzer, an advisor to the Army's Chief of Public Affairs on social media issues, said that all the units will be now be required to open access to social networking sites initially.⁵ Afterwards, if any commander does block sites for security purposes, those blocks can only be temporary.⁶ She continues, saying that the "DoD is moving away from the silly notion of having 'blacklisted' social media sites and saying, 'We're not going to lay down the

hammer and tell you where you can and cannot go, we're going to mitigate risk as it comes." ⁷

This paper first of all, concisely defines social networking. Second, examines the history of social networking. Third, addresses how social networking can serve as a change agent within the Army culture. Fourth, reviews the risks and challenges of lifting the ban on access to SNSs, and lastly, explores the benefits of leveraging social networking in the Army.

Social networking is defined as a new means of communicating and sharing information online either between two or more individuals or organizations. Social networking is the grouping of individuals into specific groups, like small rural communities or a neighborhood subdivision, if you will.⁸ Although social networking is conceivable in person, it is most popular online, primarily because the internet is filled with a lot of people sharing diverse information, themes, experiences, or professional alliances. Websites, often called social sites, are the most commonly used tool when it comes to online social networking. These websites operate like a wired community of internet customers, and commonly concentrate on certain interests, hobbies, beliefs, or views. There are still other websites (known as traditional websites) that do not focus on a hobby or view but allows anyone to contribute.

Historically, social networking as a technology, started with a type of online gathering to share information known as the Bulletin Board System (BBS). "These online meeting places were effectively independently-produced codes that allowed users to communicate with a central system where they could download files or games and post messages to other users." ⁹ BBSes continued to gain popularity throughout the

1980's and well into the 1990's, when the Internet truly kicked into gear.¹⁰ Generally, the technology related Bulletin Boards were accessed through telephone lines via a modem, and regularly nurtured the social aspects and interest-specific nature of their projects. Since telephone lines were the means of access, long distance calling charges usually applied, so many BBSes were locals-only activities. Moreover, the equipment and expertise of the period limited the flexibility of these systems, and the end-user's experience, to text-only interactions that crept along at slow speeds. Looking back to the late 1980s and the introduction of Electronic mail (email) in the place of work, social networking applications are now directing consumers away from their email inboxes and into on-line and mobile virtual communities where there is much more than email.

As social networking gained acceptance, no expert imagined the massive rise of Facebook as it is clearly the new superpower of SNSs. In fact, just to give Facebook's rapid rise some viewpoint, think of it this way: It did not exist eight years ago. Moreover, internationally, it is now one of the most popular SNSs and not just among business insiders and investors, but primarily among the average person. Due to the growth of Social networking on the internet over the last few years, it is almost impossible to find people who are not using it.

Below is the 2010 version of the annual Social Networking Map and other internet points of interest.¹¹ This map reflects the fact that social networks have dramatically increased in influence over the past few years, with new networks dominating and other networks fading into internet obscurity. The geographic area on the map indicates an approximate number of users per designated SNS and reflects Facebook's huge popularity.



Social networking can serve as a change agent within the military culture. Indeed, the pace of technological change, specifically, since the advent and attractiveness of SNSs, is creating the need for revolutionary change in organizational culture. Moreover, social networking is transforming Army culture and shifting the way information and data is passed through Army units and organizations. In fact, major change efforts have helped some organizations adapt significantly to shifting conditions, have improved the competitive standing of others, and have positioned a few for a far better future.¹² Furthermore, Army leaders are recognizing the importance of the social networking change effect and must take steps to continue to influence and shape their organizational cultures. Many familiar and prominent DoD leaders have taken to using social networking themselves, including Admiral Mike Mullen, Chairman of the Joint Chiefs of Staff. You can join him – and the over 20,000 people who follow him – on

Twitter, or check in on General Ray Odierno, Commander, Joint Forces Command on Facebook. He has close to ten thousand fans.

Even Air Force General Craig McKinley, chief of the National Guard Bureau, has become a mover and shaker across the “Twitter verse” these days. Follow and connect with him on Twitter. Gen McKinley, who penned an article late last year in “The Federal Times” entitled “Why I Tweet,” speaks frankly about how and why he embraces the wonders of Web 2.0. The chief suggests the humble 140-character tweet may soon evolve into the new commander’s coin. “When I’m traveling, I give out a lot of coins to Soldiers and Airmen who demonstrate excellence,” he said. “For the new generation, a tweet is the electronic equivalent of that coin – publicly recognizing their achievements in front of people who matter to them: their followers.”¹³

The Army supports this transformation by utilizing both embedding and reinforcing mechanisms to modernize the way it views and uses SNSs. Embedding mechanisms reflect the expectations, norms, traditions, and rules of an organization and will directly influence its principles and values. Reinforcing mechanisms are visible techniques that also influence an organizations climate, which support the stated norms, traditions and rules. For example, by using SNSs such as Facebook and Twitter, the Army regularly communicates to Soldiers and Families worldwide. Social networking sites can be a good way to make connections with people with similar interests and goals.¹⁴ Similarly, the rapid spread of social networking and media-sharing technology is also changing the conduct of military day to day operations. For instance, SharePoint and Defense Connect Online (DCO) represent a few of the changes in culture. SharePoint is a collaborative virtual work place for people to share products, ideas, find

the latest brief or published order. DCO enables users to communicate and interact with groups large and small in real-time, using high-impact presentations, web conferencing, and collaboration tools. Furthermore, to get the maximum use of the technologies and tools, the Army has built a network-centric suite of systems part of a worldwide information-sharing infrastructure, using the tools and technology of the Internet and Web to make data available any time, and any place. These are great ways to enable units to regularly conduct open and candid discussions, and have now become a routine part of Army culture.

Social networking has changed the way the Army recruits, and selects personnel.¹⁵ The Army has refined its recruitment tactics in seeking out high school and college students through the internet. In fact, the Army believes that social networking websites are an effective tool in communicating with potential recruits. Utilizing Facebook, the Army now reaches out to high school and college students on a much broader scale.

In addition to a Facebook page, the Army also maintains a Twitter page and blog, which adds a new dimension to recruitment. A blog is a type of personal Internet journal. Instead of only listening to recruiters discuss the benefits of the Army, recruiters, soldiers, and civilians are welcome to contribute in an open forum. As a result, people interested in a career in the Army can see comments from both sides of the fence, and determine whether Army culture is right for their lifestyle. In addition, social networking can advertise promotions, assignments, education, and news. Units simply share information via links, reviews, and or applications. Finally, this allows for a growing culture of information sharing, learning, and communicating.

The final topic on social networking as a change agent is to discuss another way that leaders allocate resources.¹⁶ With the advent of Army Knowledge Online (AKO), information passes up and down the chain of command much faster and more efficiently than ever before. Now at the tip of their fingers, senior leaders can strategically review personnel data on the Web, ultimately assisting in the strategic decision making process. When it comes to resources, AKO provides an online storage of soldiers' records, provides a training function, which allows soldiers and DA (Department of Army) civilians to access Army online education such as Army e-learning Program, and affords soldiers an opportunity to access their financial records, including Leave and Earning Statements, Housing allowances, and food allowances. AKO also offers a functionality for medical documentation as it maintains a soldier's medical records, including DNA, past physical exam, and status of deployment readiness.

Likewise, there are several reinforcing mechanisms to the above embedding mechanisms that affect the Army social networking transformation. The first type of reinforcing mechanism relates to the use of formal statements of organizational philosophy, creeds, and charters.¹⁷ Utilizing social media and creating websites, in addition, to placing posters and billboards throughout the unit area are reinforcing tools for what is important to the command. Consequently, the U.S. Military launched a social networking site called milBook sort of Facebook clone for organizational information. The site is more oriented towards collaboration than socialization, with the intent of providing those serving our Military the same experience they take for granted in the public domain, behind the security of a firewall.¹⁸ This networking supports broadcasted messages from leaders such as unclassified operational information, news releases,

community relations, unit history, promotions, awards, and ceremonies. The speed and transparency of information have increased dramatically and while military culture is effectively an overarching label for the military's personality, way of thinking, or values, it is just as important that senior leaders ensure that any use of embedding and reinforcing mechanisms align and remain consistent with the Army message.

There are a number of risk and challenges with using SNS sites. The decision to open military networks to these sites comes at a time when there is growing concern among leadership regarding both operational security and cyber security. Conversely, Deputy Secretary of Defense William J. Lynn III suggests in a recent DOD statement that the benefits – if handled properly – may outweigh the risks. “This directive recognizes the importance of balancing appropriate security measures while maximizing the capabilities afforded by 21st century Internet tools,” said Lynn of the DoD policy.¹⁹

Social Networking also poses major security risks from enabling avenues for cyber attacks to mistakenly exposing too much information during online chats of which may affect mission security. Additionally, social networking presents a distinctive security vulnerability known as spear phishing. This tactic allows a wily foe to troll for information on social networking sites about an actual person, and then craft an e-mail to that person to make it look like it is coming from a friend or associate. The unsuspecting victim clicks on the attachment, launching malware (short for malicious software, and is software designed to secretly access a computer system without the owner's permission) that penetrates the organization's network. Service members must also worry about spammers, scammers, and the ever-present danger of “click-jacking”—Click jacking is a malicious technique of tricking computer users into revealing

confidential information or taking control of their computer while clicking on seemingly innocent website pages or links. By this unsuspecting clicking, users could expose an entire computer network to a cyber attack. Finally, social media websites are notorious targets for cybercrime.

Contained in the new DoD policy were guidelines and a user agreement designed to address the threats of users divulging too much information on public Web pages that would enable an enemy to piece together to gain a broader vision of ongoing operations. The user agreement includes a section prohibiting the disclosure of information that could put service members at risk. In addition, the agreement prohibits “technical information, operation plans, and troop movement schedules, current and future locations of military units and ships, descriptions of overseas bases, details of weapons system or discussion of areas frequented by service members overseas.”²⁰ The user agreement states that the military can review and remove any comments it deems inappropriate, and advises users to make sure their postings are relevant to the military and do not contain threats, obscenities, sexually explicit material or any personal information.²¹

Lieutenant General William B. Caldwell, the current commander, North Atlantic Treaty Organization (NATO) Training Mission-Afghanistan, as well as, Commanding General, Combined Security Transition Command-Afghanistan, suggests the operational risks from social media are really no different than any other operational risk commanders already face. “Operational security is an enduring concern for military operations,” explained Caldwell in a recent interview with IO Sphere, the professional journal of joint information operations.²² “However, we cannot take counsel of our fears

at the expense of new media applications. As always, we must strike a balance between caution and engagement,” he continued.²³ “As new technologies continue to emerge, there will be even more challenges to the risk-benefit balance. If we surrender to our fears, we surrender a big chunk of the high media ground. Commanders accept risk in any operation. We are not talking about rejection of risk, but rather about the parameters of the risk, we’re willing to accept.”²⁴ With the emphasis senior leaders are placing on Web 2.0, (defined simply as the latest embrace of the internet for the best harnessing of collective information- sharing capabilities), I remain confident the Army will find the proper balance.”²⁵

Social networking services provide a large amount of personal information and raw data about people, organizations, and governments, which can be accessed relatively easy and anonymously. This information can then be used to target the victim. The United States military has recognized this as a concern, specifically as it relates to government employees and military service members. There have been articles in several Air Force Base newspapers discussing the risk that social networking posts can pose to operational security. According to the results of a study of 500 U.S. Air Force members with MySpace profiles, over 60% of individuals provided enough information on MySpace to make them vulnerable to a cyber-attack or blackmail—in military parlance “adversary targeting.”²⁶ To help prevent the sharing of potentially harmful information, the military has launched an education campaign to teach service members about wisely using social media platforms. The initiative is called Net Smart, and features a page on the DoD Website with tips for responsible online interactions. The site outlines threats not only to military systems but also to users’ personal information.

There are warnings about malicious code that could lead to denial of service attacks, identity theft, fraud or data theft from a government computer or network.

The U.S. Air Force is concerned about airmen's use of geolocation services like Foursquare (a location-based social networking website, software for mobile devices) and Facebook Places (Facebook's new Places feature lets users share their whereabouts with friends) and the possibility that the location services could reveal the locality of U.S. forces in war zones. In November 2010, the Air Force posted a "warning" issued on its internal Web site " to alert airmen to the potential risks of geolocation services, informing them that there may be "devastating implications for operations security and privacy" if unit or service member locations are easily pinpointed on a map.²⁷ Some geolocation services like Foursquare have responded by saying that they provide more-than-ample privacy and security settings and that if a user opts to make a check-in public rather than restricted to a group of trusted friends, that user is at his or her own risk.²⁸

In addition to the possibility of security breaks through SNSs, authorities say terrorists could use the applications in their efforts to plan an attack. Late last year, the 304th Military Intelligence Battalion at Fort Huachuca in Arizona released a draft report outlining how Twitter could be used as a tool for terrorists.²⁹ The report warned that terrorists could use Twitter via their cell phones to send and receive messages and to locate fellow cell members through links to Google Maps.³⁰ All could lead to an interruption in operations, service member identity theft, or hacking.

The mounting number of geolocation applications offered on cell phones and data devices and the greater ease with which individuals can use services like

Facebook and Twitter will aggravate traditional information-sharing complications such as assured and confidential data.

In February 2009, Representative Peter Hoekstra, R-Mich., was less cautious as he detailed via Twitter a trip to Iraq that was supposed to be kept a secret.³¹ At the time, Rep. Hoekstra was the ranking member of the House Intelligence Committee who not only publicized the trip, but also "tweeted" the whereabouts of the congressional delegation with which he was traveling. However, there is no official congressional policy in place to discourage members from publicly disclosing sensitive information about travels and whereabouts.

But even with these potential challenges, there are many benefits of leveraging social networking in the Army. First, social networking sites provide a mechanism for better communications. SNSs allow for both synchronous and asynchronous dialogue. Users can provide feedback on policy and issues of military culture. Those messages that previously would have been referred through a chain of command can now be seen directly by high-ranking members. In this case, you have the personal attention of the person you are trying to reach and are even able to have a two way communication with them. The very nature of the interaction has changed. The defining characteristic is that it is interactive— from a leader's perspective; it is choosing the information that you want, when you want it, how you want to see it.

Additionally, a growing number of deployed units have also begun using SNSs to share photographs, release official information and disseminate newsletters. Meanwhile, allowing military personnel to access social networking sites on government computers is helping to ease warfighters' minds about loved ones left at home,

according to Price Floyd, the principal deputy assistant secretary of defense for public affairs.³² In an interview on National Public Radio's (NPR) "Talk of the Nation" Floyd said soldiers are getting a boost from chatting in real-time via Skype and other services that offer video streaming or instant messaging capabilities. "Families who have gotten in touch with me talk about the tools in these Facebook sites that are an invaluable way to stay in touch with their wife, husband, brother, sister or father, even mother," said Floyd.³³ "In fact, they talk about the ability for their kids to do homework with their parent who's at war in real-time, and that kind of morale boost that happens when you're able to do that is immeasurable."³⁴

Second, leveraging social networking provides for a technologically savvy force. The Army is attempting to recruit and retain well-versed, computer literate personnel. In order to do that you cannot deny service members the capability that they can get anywhere else. Certainly, utilizing social networking will lead to better-informed service members and a current generation who are proficient and at ease navigating. Indeed, a key to successful security habits is to have talented and skilled Service members who understand network practices.

Third, the Army can leverage social networking by using it to assist in updating doctrine. Currently, the Army has begun to use social media to adapt its counterinsurgency manual with a speed that was not possible before using the technology. "Men and women who are in the field fighting in Afghanistan and Iraq are sending back and communicating with people back here in the States to update the counterinsurgency manual— how we fight counterinsurgency wars—in real time," Floyd

told his radio audience.³⁵ “We don’t have to wait several years, or until the conflict is over to do that, and we’re able to do that because of this technology.”³⁶

Fourth, the next significant aspect of leveraging social networking is the reduced costs of sharing. Overall costs to tell the Army story have been reduced while the number of people reached has increased. Simply put, previous cost used to print official recruiting and information bulletins, and pamphlets have been replaced with less expensive e-mail or online subscription services that reach a far greater audience. However, social media and electronic delivery are about more than reduced costs and increased contacts, but just as important are the relationships established with the media community.

The fifth benefit to leveraging social networking can have an immediate impact in the areas of crisis management; it can be used to put out real time, accurate, lifesaving information through platforms such as Facebook, Twitter, and other online chat mechanisms during floods, and other natural disasters. Additionally, social networking can be used during terrorist attacks for immediate, and reliable information and provide any necessary follow-on actions. Defense Secretary Robert Gates today called the freedom of communication afforded by communications technologies “a huge strategic asset for the United States.”³⁷ Meanwhile, speaking to reporters at today’s Pentagon news conference, Gates said he wants the Defense Department to take better advantage of these same technologies to reach out to the world, particularly to young people. The Secretary charged Price Floyd, the department’s new Principal Deputy Assistant Secretary for Public Affairs with enhancing the department’s outreach,

particularly to 18-to-25-year olds -- in the military, in the United States and around the world.³⁸

Navy Admiral Mike Mullen, Chairman of the Joint Chiefs of Staff, said leaders need to develop awareness about the technologies that have become almost second nature to the service members they lead. "For leaders, it's really important to be connected to that and understand it," he said, conceding that he has his own Facebook page. "I think communicating that way and moving information around that way— whether it is administrative information or information in warfare— is absolutely critical."

39

Sixth, the Army can leverage social networking to aide perhaps the most serious problem facing the force today—that is the disturbing rate of suicides. The Army cannot easily track conditions that can lead to suicide among troops, including alcohol and drug abuse, or multiple prescriptions for anti-anxiety or antidepressant drugs, because its information systems are incomplete and incompatible, according to a report released in October 2010.⁴⁰ The report, titled "Health Promotion, Risk Reduction and Suicide Prevention," said misconceptions about the restrictive nature of data privacy laws, such as the Health Insurance Portability and Accountability Act and the Privacy Act (HIPAA), complicate efforts to share soldiers' medical data with their commanders.⁴¹

Commanders need better situational awareness of risk or stress indicators for soldiers under their command to facilitate intervention. Comprehensive data can inform commanders and future actions that might be required. Leveraging social networking can eliminate stove piped data systems that preclude commanders from obtaining the kind of information they need to help troops. Hence, developing web portals with links to

multiple databases would enhance the ability to identify troops engaged in risky behavior or in need of assistance.

Lastly, the Army has begun steps of leveraging social networking from a smartphone perspective and should continue these efforts. During a limited user test in July, Soldiers received phones with the Android, Windows Mobile, or Apple operating system.⁴² The smartphones were loaded a few types of text and standard voice applications to see how the Soldiers would interact with their leadership via text messaging and voice communications. The next phase of the test expanded the use of the phones to an operational setting. The phones were equipped with more applications that provide direct voice communications and Soldier situational awareness, as well as additional reporting tools.

In addition to familiarizing themselves with the phones and applications they used for the exercise, Soldiers said they developed their own standard operating procedures (SOPs), ensuring that as a unit they were knowledgeable enough to conduct required tasks and ultimately, provide feedback. Private Harrison Henson of 1st Combat Aviation Brigade (CAB), a 2009 high school graduate, said Soldiers possess skills the Army can tap into to help develop its vision of integrating smart-phone technology in today's battlefield. "I think we're just right off the bat - for the most part - more familiar with the concept and how to work the technology," said Henson.⁴³ "What person my age doesn't text, call - whatever -- uses all the smart phones? We're already pretty familiar with it. They just enhance it and create their apps to adapt to the Army's needs." ⁴⁴

In contrast to this thorough discussion on the benefits of leveraging social networking, this paper does not address the fact that the DoD's social media policy, titled, Directive-Type Memorandum (DTM) 09-026 - Responsible and Effective Use of Internet-based Capabilities will expire on March 1, 2011.⁴⁵ Through research and dialogue with Subject Matter Experts (SMEs), the future status is unknown, especially given the most recent SECDEF efficiency efforts— could possibly be shelved indefinitely.

This uncertainty raises many unanswered questions such as will DoD continue to allow access to SNSs such as Facebook and Twitter? How will this affect communications with Family, friends, and communities? Or will the department go back to the previous status quo where they are blocked in some services but not others? It is certainly worthwhile and appropriate for DoD to revisit the policy and the reasons for continuing, modifying or ending access. There is a lot of interest in continuing a DoD-wide policy which allows its components to confidently, responsibly, securely and effectively utilize social networking.

In conclusion, leveraging social networking in the Army is a great idea as it provides for a transformation in Army culture, allow for technical innovation, better community relationships, and serve as a mechanism for shaping strategic communications. Clearly, social networking is changing the ways in which information travels around the world, it permits for improved collaboration and communications, in fact, can be a benefit to the national security community. Access to social networking sites are not only a benefit to daily operations, and strategic communications but also continue to have a positive effect on soldier moral, Senior Leaders' ability to understand

the environment, generate unity of effort, and allow units to take advantage of emerging information trends across the Department of the Army. Online social networking is a revolutionary development, giving people new ways of working and new ways of communicating. The overall effect it has had on society is good. Social networking is very popular, and from a military perspective, it is much easier to make an announcement via social media today than compared to many other facets of communications such as radio. In fact, social networking is quite influential as many people pay attention to what senior leaders comment on or state when using a social networking platform. Over the years, the social network has grown rapidly, and nowadays-small communities are able to unite members of different sex, race, creed, age, etc. When used properly, social networks can be a great way to enhance knowledge. To sum up, Deputy Secretary of Defense William J. Lynn III, who issued the implementation directive stated: "This directive recognizes the importance of balancing appropriate security measures while maximizing the capabilities afforded by 21st century Internet tools."⁴⁶ Arguably, opening the aperture on social networking was a smart decision, and leveraging social networking will continue to provide an indisputable influence on our department's organizational beliefs, values, principles and eventually, the way we live, work and communicate throughout the Army.

Endnotes

¹ Deputy Defense Secretary William J. Lynn III, "Talk to Facebook workers in Silicon Valley, Calif.," April 28, 2010, <http://www.defense.gov/news/newsarticle.aspx?id=58949> (accessed December 15, 2010).

² Chris Treadaway, Mari Smith, *Facebook Marketing: An Hour A Day* (Indianapolis, Wiley Publishing 2010), xvii.

³ U.S. Deputy Secretary of Defense, "Responsible and Effective Use of Internet-Based Capabilities," Memorandum for Secretaries of the Military Departments, Washington, DC, February 25, 2010.

⁴ Sarah Perez, "U.S. Department of Defense Goes Social...Yes, Really!" March 1, 2010, http://www.readwriteweb.com/archives/us_department_of_defense_goes_social.php (accessed December 14, 2010).

⁵ Ibid.

⁶ Ibid.

⁷ Ibid.

⁸ What Is Social Networking? "Social Networking. . . It's the way the 21st century communicates today," <http://www.whatissocialnetworking.com/> (accessed December 2, 2010).

⁹ Christopher Nickson, "The History of Social Networking," January 21, 2009, <http://www.digitaltrends.com/features/the-history-of-social-networking> (accessed October 22, 2010).

¹⁰ Ibid.

¹¹ Ethan Bloch, "The 2010 Social Networking Map," August 5, 2010, <http://www.flowtown.com/blog/the-2010-social-networking-map#ixzz18lfHV9Ug> (accessed October 22, 2010).

¹² John Kotter, *Leading Change* (Boston: Harvard Business School, 1996), 3.

¹³ GEN Craig McKinley, "Why I tweet ...Social networks transform the way we work," November 20, 2009, <http://www.federaltimes.com/article/20091120/ADOP06/911200310/1037/ADOP> (accessed November 28, 2010).

¹⁴ University of the Pacific, "Online Social Networking Dangers and Benefits," October 15, 2009, <http://web.pacific.edu/x4989.xml> (accessed December 14, 2010).

¹⁵ Ibid., 165.

¹⁶ Ibid., 164.

¹⁷ Ibid.

¹⁸ Liz Gannes, "U.S. Military Turns to Social Networking to Encourage Sharing Official and Sensitive Info," January 22, 2010, <http://gigaom.com/2010/01/22/u-s-military-turns-to-social-networking-to-encourage-sharing-official-and-sensitive-info/> (accessed October 22, 2010).

¹⁹ U.S. Deputy Secretary of Defense, "Responsible and Effective Use of Internet-Based Capabilities,"

²⁰ Department of Defense, "DoD Social Media Hub," <http://socialmedia.defense.gov/> (accessed December 14, 2010).

²¹ Ibid.

²² Lieutenant General William B. Caldwell IV, "On New Media in Military Operations," IO Sphere Online, Summer 2009, http://www.au.af.mil/info-ops/iosphere/09summer/iosphere_summer09_caldwell.pdf (accessed December 14, 2010).

²³ Ibid.

²⁴ Ibid.

²⁵ Ibid.

²⁶ Jeffery Carr, *Inside Cyber Warfare* (Sebastopol, O'Reilly Media 2009), 93.

²⁷ Caroline McCarthy, "Air Force Worried Geolocation Services Help Enemy," November 17, 2010 http://news.cnet.com/8301-13577_3-20023168-36.html#ixzz18mpMQTPp (accessed December 14, 2010).

²⁸ Ibid.

²⁹ Hollis Templeton, "Social media benefits trump security fears", June 10, 2009, <http://news.medill.northwestern.edu/washington/news.aspx?id=133987> (accessed February 4, 2011)

³⁰ Ibid.

³¹ Ibid.

³² Price Floyd, Principal Deputy Assistant Secretary of Defense for Public Affairs, "Will The Military Friend Facebook Anytime Soon?" NPR interview on Talk of the Nation show, September 22, 2009, <http://www.npr.org/templates/story/story.php?storyId=113073687> (accessed December 2, 2010).

³³ Ibid.

³⁴ Ibid.

³⁵ Ibid.

³⁶ Ibid.

³⁷ Defense Secretary Gates and Chairman of the Joint Chiefs of Staff, ADM Mullen, "Communications Technologies 'Strategic Asset' for United States," June 18, 2009, <http://www.defense.gov/news/newsarticle.aspx?id=54834> (accessed December 14, 2010).

³⁸ Ibid.

³⁹ Ibid.

⁴⁰ U.S. Army, *Army Health Promotion, Risk Reduction, Suicide Prevention* (Washington, DC: Office of Vice Chief of Staff, July 2010), 235.

⁴¹ Ibid.

⁴² Lt. Col Deanna Bague, "Soldiers test smart phones in field exercise," December 14, 2010, <http://www.army.mil/-news/2010/12/14/49409-soldiers-test-smart-phones-in-field-exercise/> (accessed December 15, 2010).

⁴³ Ibid.

⁴⁴ Ibid.

⁴⁵ U.S. Deputy Secretary of Defense, "Responsible and Effective Use of Internet-Based Capabilities".

⁴⁶ Ibid.